

Symantec™ Relay for HP OpenView Operations Integration Guide



Symantec™ Relay for HP OpenView Operations Integration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.
Documentation version 1.0

Copyright Notice

Copyright © 2003 Symantec Corporation.
All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. SESA, Symantec Enterprise Security Architecture, and Symantec Security Response are trademarks of Symantec Corporation. OpenView® and VantagePoint® are registered U.S. trademarks of Hewlett-Packard Company.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32- and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

UNIX® is a registered trademark of the Open Group.

Sun™, Java™, and Solaris™ are U.S. trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

MS-DOS® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape and the Netscape N and Ship's Wheel logos are registered trademarks of Netscape Communications Corporation in the U.S. and other countries.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged. Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
 - Error messages/log files
 - Troubleshooting performed prior to contacting Symantec
 - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT

Symantec Relay for HP OpenView Operations

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use each copy of the Software, indicated in the License Module, on up to two computers and a single handheld device as set forth in the documentation If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;

D. use the Software in accordance with any written agreement between You and Symantec; and

E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

A. copy the printed documentation that accompanies the Software;

B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompiler, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;

D. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor

G. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance

hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of the Software to any entity not authorized by or specifically prohibited by the United States Federal Government is strictly prohibited.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and

Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Technical support

Chapter 1	Introducing the Symantec Relay for HP OpenView Operations	
	Who should read this guide	11
	What you should know	11
	About the Symantec Relay for HP OpenView Operations	12
	How the Symantec Relay for HP OpenView Operations processes events	14
	Symantec Relay for HP OpenView Operations CD contents	15
Chapter 2	Installing the Symantec Relay for HP OpenView Operations	
	Installation overview	17
	Before you install	18
	Verifying that SNMP services are installed on the SESA Manager computer	18
	Verifying that SNMP properties are correctly configured in the SESA Console	18
	System requirements	20
	Installing the Symantec Relay for HP OpenView Operations	21
	Configuring HP OpenView Operations to receive alerts from SESA	24
	Adding the SESA Manager node to the SESA Servers node group in HP OpenView Operations for UNIX	24
	Adding the SESA Manager node to the SESA Servers node group in HP OpenView Operations for Windows	27
	Configuring alerts in the SESA Manager	28
	Filtering criteria for a particular event class	32
	How SESA alert severities correspond to HP OpenView Operations message severities	34

- Uninstalling the Symantec Relay for HP OpenView Operations 35
 - Uninstalling the HP OpenView Operations agent from the SESA Manager 35
 - Uninstalling the Symantec Relay for HP OpenView Operations software from a Windows computer 36
 - Uninstalling the Symantec Relay for HP OpenView Operations software from a UNIX computer 37

Chapter 3

Testing, using, and troubleshooting the Symantec Relay for HP OpenView Operations

- Testing Symantec Relay for HP OpenView Operations operation 41
 - Verifying that SESA can successfully generate an alert 42
 - Verifying that SESA configuration components appear in the HP OpenView Operations Console 43
 - Verifying that SESA alerts appear in the HP OpenView Operations Console 45
- Launching the SESA Console in HP OpenView Operations 47
 - Launching the SESA Console in HP OpenView Operations for Windows 47
 - Launching the SESA Console in HP OpenView Operations for UNIX 48
- Troubleshooting the Symantec Relay for HP OpenView Operations 49
 - Distributing a configuration change manually in SESA 50

Index

Introducing the Symantec Relay for HP OpenView Operations

This chapter includes the following topics:

- [Who should read this guide](#)
- [What you should know](#)
- [About the Symantec Relay for HP OpenView Operations](#)
- [How the Symantec Relay for HP OpenView Operations processes events](#)
- [Symantec Relay for HP OpenView Operations CD contents](#)

Who should read this guide

This guide is intended for HP OpenView administrators and SESA administrators who will install, configure, and use the Symantec Relay for HP OpenView Operations.

What you should know

You should have prior knowledge of HP OpenView Operations for Windows or HP OpenView Operations for UNIX, depending on the computer platforms in your networking environment. You should also be familiar with basic SESA operation and event logging.

For more information, see the *Symantec Enterprise Security Architecture Installation Guide* and the *Symantec Enterprise Security Architecture Administrator's Guide*.

About the Symantec Relay for HP OpenView Operations

SESA is an event management system that collects data from events generated by security products. SESA categorizes events into classes such as antivirus, content filtering, network security, and systems management. The range of events varies depending on the security products that integrate with SESA.

The events conform to an extensible family of event classes and types, which are defined by sets of XML schema. Once collected, event information is stored in the SESA DataStore for access by SESA management functions through the SESA Console.

The Symantec Relay for HP OpenView Operations is an HP OpenView-certified Smart Plug-In (SPI) that lets HP OpenView Operations receive events that originate from SESA sources. Like all SPIs, the Symantec Relay for HP OpenView Operations installs the configuration components in HP OpenView Operations.

Table 1-1 lists the SESA configuration components that the Symantec Relay for HP OpenView Operations installs.

Table 1-1 SESA configuration components installed by the Symantec Relay for HP OpenView Operations

Components shown in HP OpenView Operations for Windows	Components shown in HP OpenView Operations for UNIX	Description
SESA Servers node group	SESA Servers node bank	<p>The SESA Servers node group or bank contains the SESA Manager computers that are HP OpenView Operations managed nodes. A computer becomes a managed node when the HP OpenView Operations agent is installed on it.</p> <p>After the administrator adds the SESA Servers node group or bank, the SESA SNMP Alerts policy (otherwise known in HP OpenView Operations as an SNMP Interceptor policy) is automatically deployed to the node, which allows HP OpenView Operations to receive alerts from SESA.</p>

Table 1-1 SESA configuration components installed by the Symantec Relay for HP OpenView Operations

Components shown in HP OpenView Operations for Windows	Components shown in HP OpenView Operations for UNIX	Description
SPI for SESA policy group	SESA SPI template group	SPI for SESA policy groups or SESA SPI template groups let HP OpenView Operations receive and process messages from different sources. When a relayed alert is caught by the SESA SNMP Alerts policy or template, HP OpenView Operations applies several rules to the Symantec SESA Servers node group or bank, and populates a new HP OpenView Operations message using the information from the SNMP trap.
SESA Administrators user role	SESA Administrators user role	The SESA Administrators user role has permissions to view SESA messages (alerts relayed from SESA), run the Launch SESA Console tool or application, and manage the nodes in the Symantec SESA Servers node group or bank. The SESA Administrators user role provides HP OpenView Operations administrators with an easy way to assign SESA management privileges to the users in the organization who are responsible for security and SESA administration.
SESA Console tool	SESA Console application	The SESA Console tool or application lets administrators launch one or more SESA Consoles from HP OpenView Operations. When invoked, the SESA Console uses the list of one or more nodes to launch a Web browser with the URL of the SESA Console for each chosen node.
SESA Messages	SESA Messages message group	The SESA Messages message group lets administrators view alerts relayed from SESA.

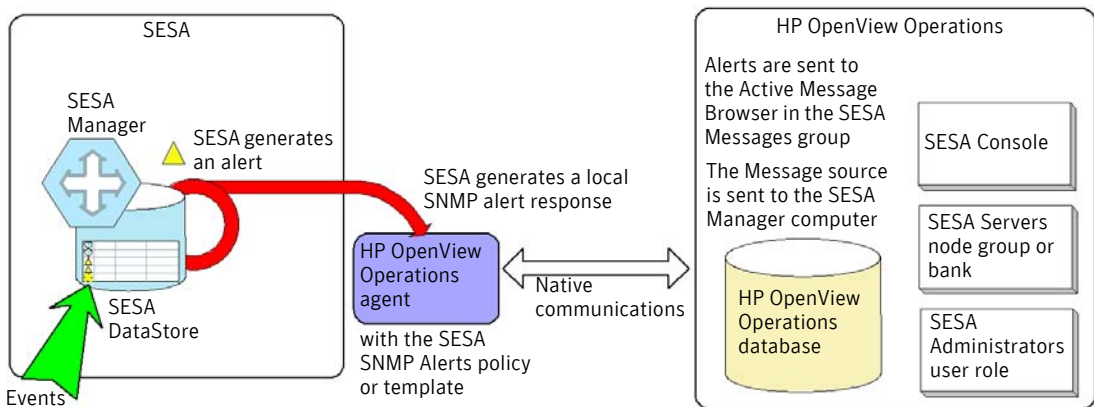
After Symantec Relay for HP OpenView Operations installation, the configuration components are uploaded to the active HP OpenView Operations configuration.

How the Symantec Relay for HP OpenView Operations processes events

The Symantec Relay for HP OpenView Operations captures events that are sent to SESA, maps these events to the proper format for the HP OpenView Operations environment, and forwards the events to HP OpenView Operations.

[Figure 1-1](#) shows the main components of the Symantec Relay for HP OpenView Operations and indicates the flow of event data through those components.

Figure 1-1 Symantec Relay for HP OpenView Operations components



The data flow begins with event data from a SESA-enabled security product. The SESA Agent that is installed on the security product computer sends event data to the SESA Manager. Once the event data is validated and saved to the SESA DataStore, SESA can generate an alert if the event data has been configured in SESA to trigger an alert. The alert is configured to generate an SNMP response locally.

When the Symantec Relay for HP OpenView Operations is installed, an HP OpenView Operations agent runs on the SESA Manager computer and is configured with the SESA SNMP Alerts policy or template. The policy or template filters and formats the SNMP response (the alert). By default, policy or template rules cause the HP OpenView Operations for Windows agent to discard informational alerts with a severity of 1 prior to transmission to HP OpenView

Operations. However, you can customize the rule to forward informational alerts as necessary.

However, if the alert has a severity of 2 or greater, an HP OpenView Operations message is generated and the HP OpenView Operations agent sends the message to the HP OpenView Operations management server.

Symantec Relay for HP OpenView Operations CD contents

[Table 1-2](#) describes the folders and files that the Symantec Relay for HP OpenView Operations CD contains.

Table 1-2 Symantec Relay for HP OpenView Operations CD contents

Folders and Files	Description
\SRFHPOVO.PDF	<i>Symantec Relay for HP OpenView Operations Integration Guide</i>
\OVO_Unix_SPI\SESA_SPI.depot	Symantec Relay for HP OpenView Operations installation depot
\OVO_Unix_SPI\README.TXT	Symantec Relay for HP OpenView Operations Readme file for HP OpenView Operations for UNIX
\OVO_Windows_SPI\Symantec Relay for HP OpenView Operations.msi	Symantec Relay for HP OpenView Operations installation program
\OVO_Windows_SPI\README.TXT	Symantec Relay for HP OpenView Operations Readme file for HP OpenView Operations for Windows

Installing the Symantec Relay for HP OpenView Operations

This chapter includes the following topics:

- [Installation overview](#)
- [Before you install](#)
- [System requirements](#)
- [Installing the Symantec Relay for HP OpenView Operations](#)
- [Configuring HP OpenView Operations to receive alerts from SESA](#)
- [Configuring alerts in the SESA Manager](#)
- [Uninstalling the Symantec Relay for HP OpenView Operations](#)

Installation overview

You must perform the following separate sets of procedures to install and configure the Symantec Relay for HP OpenView Operations to relay alerts from SESA to HP OpenView Operations:

- [Installing the Symantec Relay for HP OpenView Operations](#)
- [Configuring HP OpenView Operations to receive alerts from SESA](#)
- [Configuring alerts in the SESA Manager](#)

Before you install

Before you install the Symantec Relay for HP OpenView Operations, make sure that the SESA Manager, SESA Directory, SESA DataStore, and the HP OpenView Operations management server are installed and running.

In addition, make sure that the SNMP service is installed and operating on the SESA Manager computer and that it is configured properly in the SESA Console. HP OpenView Operations version 7.1 uses SNMPv1 by default. It requires an update for SNMPv2.

Verifying that SNMP services are installed on the SESA Manager computer

You can check the Services window of Microsoft Windows to verify that SNMP services are installed and running on the SESA Manager computer.

If the SNMP services are not installed, you can use the Add/Remove Programs feature in Windows to install them.

For more information on using Add/Remove Programs, see the Microsoft Windows documentation.

To verify that SNMP services are installed on the SESA Manager computer

- 1 On the SESA Manager computer, on the Windows taskbar, click **Start** > **Control Panel**.
- 2 In the Control Panel window, click **Administrative Tools**.
- 3 In the Administrative Tools window, click **Services**.
- 4 In the Services window, verify that the following services are installed and started:
 - SNMP Service
 - SNMP Trap Service

Verifying that SNMP properties are correctly configured in the SESA Console

The Symantec Relay for HP OpenView Operations uses the native SNMP alerting feature in the SESA Manager to relay alerts to the HP OpenView Operations management server. You must verify that the SNMP properties are correctly configured in the SESA Console.

To verify that the SNMP properties are correctly configured in the SESA Console

- 1 Do one of the following:
 - If you are physically at the SESA Manager computer, on the Windows taskbar, click **Start > Programs > Symantec Enterprise Security > SESA Console**.
 - If you are not at the SESA Manager computer, in an Internet browser, type **https://<IP address or FQDN of SESA Manager computer>/sesa/ssmc**
- 2 Log on to the SESA Console using the rights of the SESA Domain Administrator.
- 3 In the SESA Console, on the Configurations view tab, in the left pane, expand **SESAv1.1 > SESA Manager Components Configuration**.
- 4 Under SESA Manager Components Configuration, click **Default**.
- 5 In the right pane, on the SNMP tab, verify that the following properties are set to the indicated values:

Host	LocalHost
Port	162
Community	Public
VersionOne	true (for SNMPv1) false (for SNMPv2)

- 6 Make any changes as necessary.

If possible, use SNMPv1. If your networking environment requires you to use SNMPv2, you must first update the HP OpenView Operations for Windows agent to use SNMPv2. Depending on your HP OpenView Operations platform, you may need to install patches or otherwise configure HP OpenView Operations.

For more information on setting up HP OpenView Operations for UNIX or HP OpenView Operations for Windows to use SNMPv2, see the HP OpenView Operations documentation or visit the HP OpenView Web site.
- 7 Click **Apply**.

System requirements

Table 2-1 lists the system requirements for an HP OpenView Operations management server that is running the Symantec Relay for HP OpenView Operations.

Table 2-1 HP OpenView Operations management server system requirements

Component	System requirement
Symantec Relay for HP OpenView Operations	25 KB of hard disk space
HP OpenView Operations for Windows version 7.1	Windows 2000 Server/Advanced Server with Service Pack 2 and the latest Microsoft security patches
HP OpenView Operations for UNIX version 7.1	<ul style="list-style-type: none">■ Sun Solaris 2.7 or 2.8■ HP-UX 11.0 or 11.11

Table 2-2 lists the system requirements for a SESA Manager computer that is a managed node for HP OpenView Operations.

Table 2-2 Managed node computer requirements for the SESA Manager

Component	System requirement
HP OpenView Operations agent	<ul style="list-style-type: none">■ 18 MB of memory■ 75 MB of hard disk space; 100 MB recommended
SESA Manager computer operating system	Windows 2000 Server/Advanced Server with Service Pack 2 and the latest Microsoft security patches
SESA software	<p>SESA version 1.1 with the most current patches applied</p> <p>If you have a 1.1.x version of SESA, you can run LiveUpdate to update SESA 1.1.x with the most current patches. If you have a 1.0.x version of SESA, you must first uninstall it before you can install version 1.1.x. You cannot migrate 1.0.x versions of SESA to version 1.1 or reinstall over 1.0.x versions. Version 1.1.x is not backward-compatible.</p> <p>For more information, see the <i>Symantec Enterprise Security Architecture Installation Guide</i>.</p>

Note: Do not install SESA components on a computer that is also functioning as an Active Directory Domain Controller.

Installing the Symantec Relay for HP OpenView Operations

This installation assumes that all SESA components are operating properly. The Symantec Relay for HP OpenView Operations is installed on the computer that hosts the HP OpenView Operations management server.

Install the Symantec Relay for HP OpenView Operations

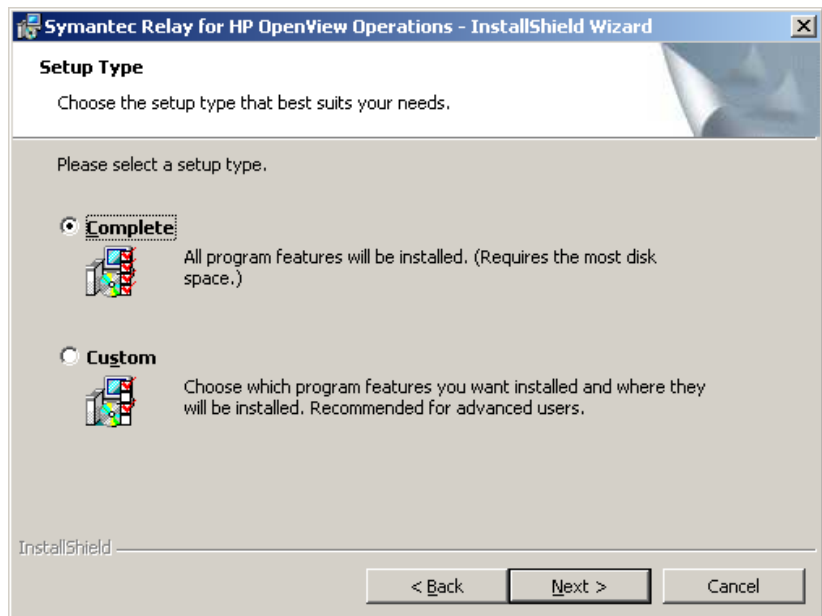
The installation procedure varies depending on whether you are installing on HP OpenView Operations for Windows or HP OpenView Operations for UNIX. You use a Windows Installation Wizard for the Windows version, while you use the HP Software Distributor tool for the UNIX version.

Note: If you are installing on UNIX platforms, make sure that HP OpenView Operations Motif GUI is closed prior to installing the Symantec Relay for HP OpenView Operations software.

To install the Symantec Relay for HP OpenView Operations for Windows software on Windows platforms

- 1 On the HP OpenView Operations for Windows management server, insert the Symantec Relay for HP OpenView Operations CD into the CD-ROM drive.
- 2 Open Windows Explorer, and navigate to the OVO_Windows_SPI directory on the CD.
- 3 Double-click **Symantec Relay for HP OpenView Operations.msi** to start the Windows Installation Wizard.

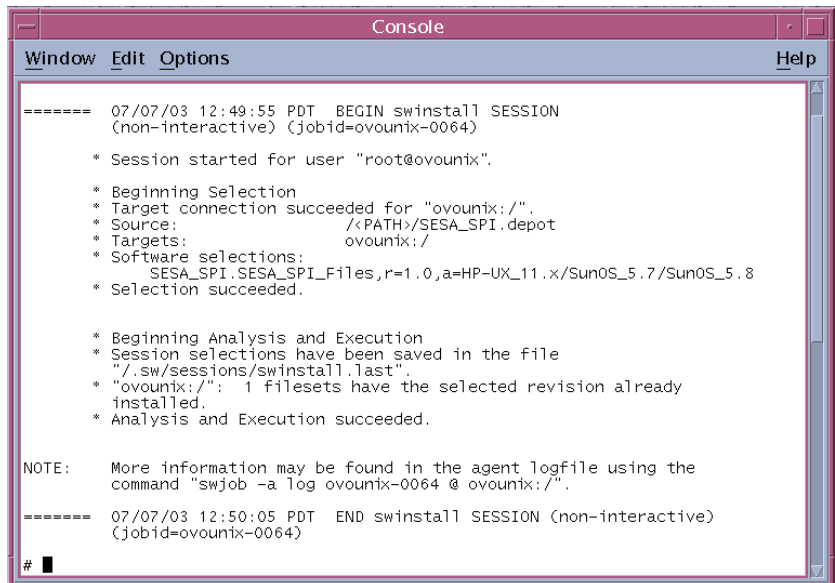
- 4 Follow the on-screen instructions until you see the Setup Type window.



- 5 In the Setup Type window, do one of the following:
 - To install the software to default locations, click **Complete**, then click **Next**.
 - To install the software to a location other than the default, click **Custom**, then click **Next**.
- 6 Continue following the on-screen instructions to install the software.
- 7 When the wizard completes, click **Finish**.

To install the Symantec Relay for HP OpenView Operations for UNIX software on Sun Solaris or HP-UX platforms

- 1 On the HP OpenView Operations for UNIX management server, insert the Symantec Relay for HP OpenView Operations CD into the CD-ROM drive.
- 2 If necessary, log in to the HP OpenView Operations management server using appropriate administrative privileges.
- 3 Open the UNIX Console or Terminal window.
- 4 If necessary, mount the Symantec Relay for HP OpenView Operations CD.
- 5 In the UNIX Console or Terminal window, at the command prompt, type the following script:
swinstall -s /<full path>/SESA_SPI.depot SESA_SPI @ <Host computer name>
<Host computer name> is the host name of the HP OpenView Operations management server.
- 6 Press **Enter**.



```
Console
Window Edit Options Help

===== 07/07/03 12:49:55 PDT .BEGIN swinstall SESSION
(non-interactive) (jobid=ovounix-0064)

* Session started for user "root@ovounix".

* Beginning Selection
* Target connection succeeded for "ovounix:/".
* Source: /<PATH>/SESA_SPI.depot
* Targets: ovounix:/
* Software selections:
  SESA_SPI,SESA_SPI_Files,r=1.0,a=HP-UX_11.x/SunOS_5.7/SunOS_5.8
* Selection succeeded.

* Beginning Analysis and Execution
* Session selections have been saved in the file
"/.sw/sessions/swinstall.last".
* "ovounix/": 1 filesets have the selected revision already
installed.
* Analysis and Execution succeeded.

NOTE: More information may be found in the agent logfile using the
command "swjob -a log ovounix-0064 @ ovounix:/".

===== 07/07/03 12:50:05 PDT .END swinstall SESSION (non-interactive)
(jobid=ovounix-0064)

# █
```

Configuring HP OpenView Operations to receive alerts from SESA

After you install the Symantec Relay for HP OpenView Operations software, you can configure HP OpenView Operations to receive alerts from the SESA Manager. To configure HP OpenView Operations, you do the following:

- Set up the SESA Manager computer to be a managed node in HP OpenView Operations.
For information on setting up managed nodes in HP OpenView Operations, see the HP OpenView Operations documentation.
- Add the SESA Manager node to the SESA Servers node group in HP OpenView Operations.
 - If your HP OpenView Operations management server runs on the Sun Solaris or HP-UX operating system, adding the SESA Manager node to the SESA Servers node group also involves adding the SESA Administrators role to any HP OpenView Operations users who will be administering SESA, and distributing the SESA SPI template to the SESA Manager computer.
See [“Adding the SESA Manager node to the SESA Servers node group in HP OpenView Operations for UNIX”](#) on page 24.
 - If your HP OpenView Operations management server runs on the Windows operating system, you add the SESA Manager node to the SESA Servers node group.
See [“Adding the SESA Manager node to the SESA Servers node group in HP OpenView Operations for Windows”](#) on page 27.

Adding the SESA Manager node to the SESA Servers node group in HP OpenView Operations for UNIX

After you install the Symantec Relay for HP OpenView Operations software, you can configure HP OpenView Operations for UNIX to receive alerts from the SESA Manager. Configuration involves adding the SESA Manager node to the SESA Servers node group in HP OpenView Operations for UNIX.

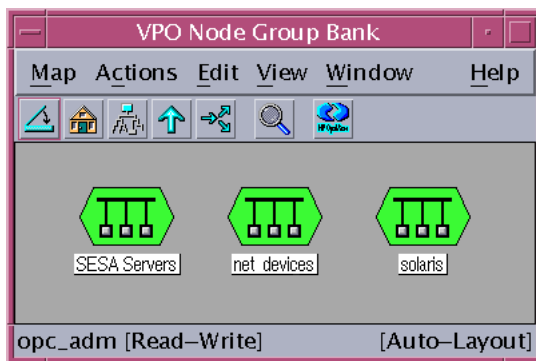
Add the SESA Manager node to the SESA Servers node group in HP OpenView Operations for UNIX

To add the new SESA Manager node to the SESA Servers node group in HP OpenView Operations for UNIX, you perform the following procedures:

- Activate the SESA Manager node as a SESA Server node in HP OpenView Operations for UNIX.
- Distribute the SESA SPI template to the SESA Manager node.
- Add the SESA Administrators role to any HP OpenView Operations users who will be administering SESA.

To activate the SESA Manager node as a SESA Server node in HP OpenView Operations for UNIX

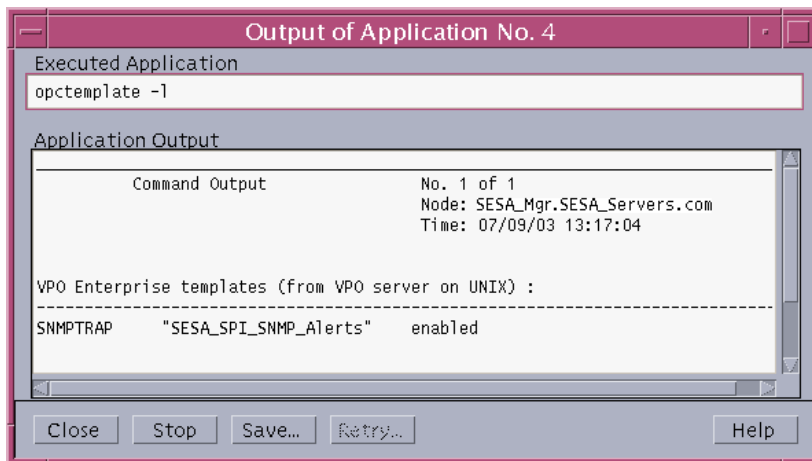
- 1 On the HP OpenView Operations management server, log in to HP OpenView Operations for UNIX using appropriate administrative privileges.
- 2 In the VPO Node Banks window, on the Window menu, click **Node Group Bank**.



- 3 In the VPO Node Group Bank window, double-click **SESA Servers**.
- 4 In the VPO Node Banks window, use a drag-and-drop operation to move the SESA Manager computer that you need to the SESA Servers node group in the VPO Node Group Bank window.

To distribute the SESA SPI template to the SESA Manager node

- 1 On the HP OpenView Operations management server, in the VPO Node Bank window, on the Actions menu, click **Agents > Install Update SW & Config**.
 - 2 In the Install/Update VPO Software and Configuration window, under Components, check **Templates**, then click the **OK** button.
 - 3 In the VPO Node Bank window, on the Window menu, click **Application Bank**.
 - 4 In the Application Bank window, double-click the **NT Tools** symbol to open the Application Group: NT Tools window.
 - 5 In the VPO Node Bank window, use a drag-and-drop operation to move the SESA Manager computer symbol to the VPO Templates symbol in the Application Group: NT Tools window.
 - 6 In the Output of Application window, ensure that the SESA_SPI_SNMP_Alerts template is enabled.
- An enabled template indicates that it has been installed successfully.



To add the SESA Administrators role to any HP OpenView Operations users who will be administering SESA

- 1 On the HP OpenView Operations management server, in the VPO Node Banks window, on the Window menu, click **User Bank**.
- 2 In the User Bank window, on the Actions menu, click **User > Modify**.

- 3 In the Modify User window, click the **Profiles** button.
- 4 In the Profiles of User window, on the Window menu, click **User Profile Bank**.
- 5 In the User Profile Bank window, use a drag-and-drop operation to move the SESA Administrators profile to the Profiles of User window.

Adding the SESA Manager node to the SESA Servers node group in HP OpenView Operations for Windows

After you install the Symantec Relay for HP OpenView Operations software, you can configure HP OpenView Operations for Windows to receive alerts from the SESA Manager. Configuration involves adding the SESA Manager node to the SESA Servers node group. Once the SESA Manager node is added to the group, the SESA_SPI policy is activated.

To add the SESA Manager node to the SESA Servers node group in HP OpenView Operations for Windows

- 1 On the HP OpenView Operations management server, log on to HP OpenView Operations for Windows using an account that has administrative privileges to the SESA Manager.
- 2 On the Windows taskbar, click **Start > Programs > HP OpenView > Console**.
- 3 In the Connect To Server window, type the name of the computer on which the management server is installed.
- 4 Click **Finish**.
- 5 In the HP OpenView Operations Console, in the console tree, on the toolbar, click the Node Configuration Editor symbol.
- 6 In the Configure Managed Nodes dialog box, in the right pane, select the SESA Manager computer, then use a drag-and-drop operation to move it to the SESA Servers node group.
- 7 In the Node Properties dialog box, configure the new node.
If you don't know what a particular box requires, click the **Help** button for additional information.
- 8 Click **Apply** as you finish with each tab to apply your changes.
- 9 Click **OK** to confirm your changes and close the dialog box.
The SPI for SESA policy is automatically deployed to the SESA Server node.

Configuring alerts in the SESA Manager

Before SESA can relay alerts to HP OpenView Operations, you must create at least one alert configuration in the SESA Console. Alert configurations instruct SESA how and when to generate alerts based on events in a SESA DataStore. When you create an alert configuration, you can select filtering criteria such as event name, event class, product, and frequency. You can also specify the type of notification that you want to send for the alert once the event or events satisfy the filtering criteria to trigger it.

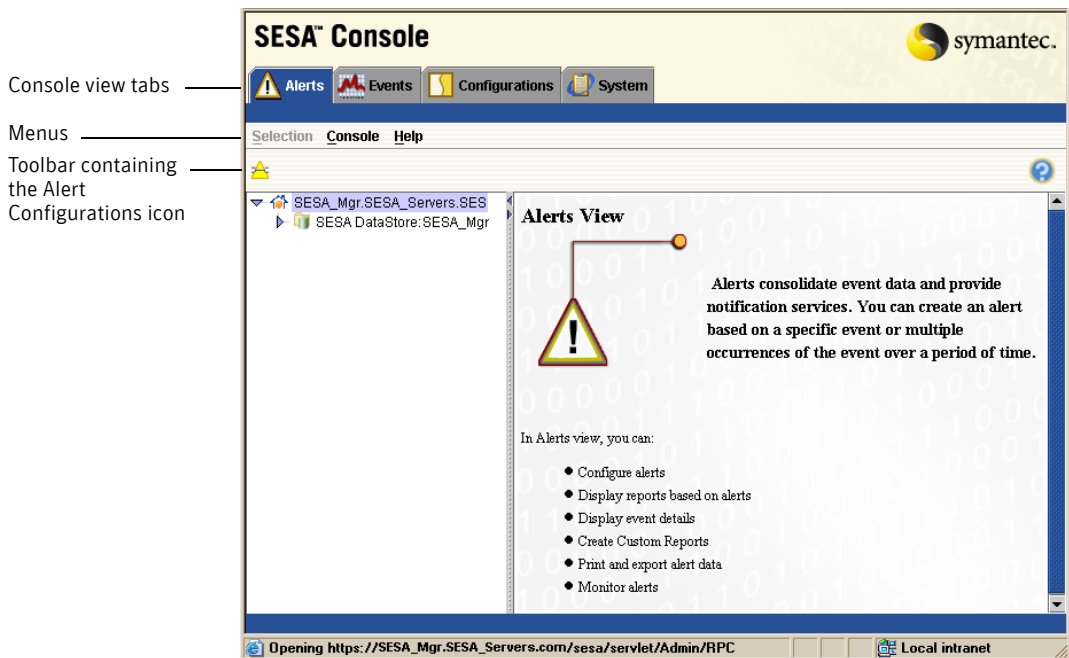
To configure an alert that SESA can relay to HP OpenView Operations, you must specify at least the following criteria:

- Alert name
- Alert description
- Alert severity of 2 or more
- Notification by SNMP trap

You can create alert configurations by completing a Create a new Alert Configuration Wizard for each type of alert that you want to relay to HP OpenView Operations from SESA. The wizard is located in the SESA Console on the Alerts view tab.

[Figure 2-1](#) shows the main features of the SESA Console window with the Alerts view tab active.

Figure 2-1 SESA Console window with the Alerts view tab active



If you have not yet configured any alerts in the SESA Console, you may want to review the various ways of configuring them in SESA.

For more information, see the *Symantec Enterprise Security Architecture Administrator's Guide*.

To create an alert configuration using the wizard

- 1 Do one of the following to access the SESA Console:
 - On the SESA Manager computer, on the Windows taskbar, click **Start > Programs > Symantec Enterprise Security > Console**.
 - On a computer that has access to the SESA Manager computer using the HTTPS protocol, in an Internet browser, in the Address text box, type the URL of the SESA Manager computer, then press **Enter**.
 For example, <https://SESAManagerDomainName/sesa/ssmc>
 You can use an IP address in place of a domain name.
 For more information on logging on to the SESA Console, see the *Symantec Enterprise Security Architecture Administrator's Guide*.
- 2 In the Logon window, log on to the SESA Console using a SESA account that has sufficient rights to modify SESA configurations.
- 3 In the SESA Console, on the Alerts view tab, on the toolbar, click the Alert Configurations icon.
- 4 In the Alert Configurations window, on the toolbar, click **New (+)**.
- 5 In the initial dialog box of the Create a new Alert Configuration Wizard, click **Next**.

Create a new Alert Configuration Wizard

General

Type the **Alert Configuration name**, select the **Alert severity**, and provide an **Alert description**.

★ **Alert Configuration name**

Alert description

Alert severity

2 - Warning

DataStores

☒ SESA DataStore: MyDataStore

★ **Required**

<< Back Next >> Cancel

Java Applet Window

- 6 In the General dialog box, do the following:
 - Type a name and description for the alert configuration.
You must type both a name and description when you need an alert notification by SNMP trap. Otherwise, SESA cannot relay the alert successfully.
 - Select an alert severity of 2 - Warning or greater.
By default, HP OpenView Operations does not receive alerts with severities of less than 2.
SESA alert severities vary slightly from message severities in HP OpenView Operations.
See [“How SESA alert severities correspond to HP OpenView Operations message severities”](#) on page 34.
 - Select a SESA DataStore.
One or more DataStores may be available. If only one DataStore is available, it is already selected and cannot be changed. Selecting a DataStore determines both where the events that will trigger the alert are logged and where the alert that occurs because of this configuration will be logged.
- 7 Click **Next**.
- 8 In the Event Information dialog box, select one or more event filtering criteria to restrict the events for which the alert is based.
- 9 If you want to further restrict criteria based on the event class that you have selected in the Event Information dialog box, click **Advanced**.
The criteria that you select in both the Event Information and Event Filter (Advanced) dialog boxes cannot be changed later by editing the alert. If you do not make selections now, the default settings are used. Using all default settings means that all events are used to generate the alert. The more selections that you make, the more finely tuned the alert is.
See [“Filtering criteria for a particular event class”](#) on page 32.
- 10 Click **Next**.
- 11 In the Thresholds and Frequencies dialog box, do one of the following:
 - Specify an alert threshold and alert frequency, then click **Next**.
 - Click **Next** to accept the default settings to create an alert for every occurrence of the event.

You can specify an alert threshold and frequency later by editing the alert configuration.

For more information, see the *Symantec Enterprise Security Architecture Administrator's Guide*.

- 12 In the Users to Notify dialog box, do one of the following:
 - Click **Next** to relay the alert to HP OpenView Operations without notifying any users.
You can add users later by editing the alert configuration.
 - Click **Add** to add users to be notified when the event occurs in SESA, then click **Next**.
- 13 In the Additional Notifications dialog box, click **Click here to enable SNMP trap message responses for this alert**, then click **Next**.
- 14 In the Alert Configuration Summary dialog box, review the information that you have specified, then do one of the following:
 - Click **Back** and make any changes as necessary.
 - Click **Finish** to create the alert configuration.
The Task/Status list at the bottom of the dialog box scrolls up to show the properties that SESA is creating. A green check mark indicates success.
- 15 When the Cancel button changes to a Close button, click **Close**.
When the Alert Configurations window reappears, the new alert configuration appears in the left pane.

Filtering criteria for a particular event class

To further restrict the types of conditions for a particular event class that can trigger an event, you can use the Event Filter (Advanced) dialog box in the Create a new Alert Configuration Wizard. This dialog box is also available outside of the Create a new Alert Configuration Wizard.

For more information on the Event Filter (Advanced) dialog box, see the *Symantec Enterprise Security Architecture Administrator's Guide*.

The criteria that you select in the Event Filter (Advanced) dialog box cannot be changed later by editing the alert. If you do not make any selections, the default settings are used. Using all default settings means that all events in the event class are used to generate the alert. The more selections that you make, the more finely tuned the alert is.

To filter criteria for a particular event class

- 1 In the Create a new Alert Configuration Wizard, in the Event Information dialog box, click **Advanced**.

- 2 In the Event Filter (Advanced) dialog box, under Available Common Event Columns, select an event column.
Common event columns are available for all events, regardless of event class.
- 3 Under Value, do one of the following to specify a value for the common event column that you selected:
 - Click the ellipses control (...) to select a value from the defined set of values in the SESA DataStore for your selected event column.
An ellipses control only appears when an event column has defined values. For example, if you click Machine as the common event column, you can click the ellipses control, then select a value from a list of the computers that are defined in the SESA Directory for your security network.
 - Type the value, using alphanumeric characters.
For your entry to be meaningful, you must type the value exactly as it is stored in the SESA DataStore. For example, the case that you use must match the case that is used in the DataStore.

To determine the exact alphanumeric format, you can look at a report of an event that contains the column.

For more information on how to display event reports, see the *Symantec Enterprise Security Architecture Administrator's Guide*.

- 4 Under Available Event Class Columns, select another event class column if one is available and you want to further restrict the alerting criteria. Depending on the restrictions that you have already selected, this option may not be available.
- 5 If you selected an event class column, under Value, type a value. If the column you that select has a defined set of values in the SESA DataStore, an ellipses control is available to help you select a value.
- 6 Click **OK** to apply changes and return to the Event Information dialog box in the Create a new Alert Configuration Wizard.











How SESA alert severities correspond to HP OpenView Operations message severities

The severity levels of alerts in SESA differ slightly from the severity levels of messages in HP OpenView Operations. In SESA, event severities are set independently from alert severities. For example, a critical event can be set to generate an informational alert.

By default, HP OpenView Operations does not relay informational messages. In addition, both a critical and fatal alert in SESA are recognized as a critical message in HP OpenView Operations.

Table 2-3 lists SESA alert severities and describes how they correspond to HP OpenView Operations message severities.

Table 2-3 How SESA alerts map to HP OpenView Operations messages

SESA Windows symbol	SESA alert severity	HP OpenView Operations for Windows symbol	HP OpenView Operations for UNIX symbol	HP OpenView Operations Message severity
	2 - Warning		Warn	Warning
	3 - Minor		Min	Minor
	4 - Major		Maj	Major
	5 - Critical		Crit	Critical
	6 - Fatal		Crit	Critical

Uninstalling the Symantec Relay for HP OpenView Operations

Removing the Symantec Relay for HP OpenView Operations involves removing the HP OpenView Operations agent from the SESA Manager computer and the Symantec Relay for HP OpenView Operations software from the appropriate HP OpenView Operations management servers. You can perform these tasks in any sequence.

Uninstalling the HP OpenView Operations agent from the SESA Manager

You use the Windows Add/Remove Programs feature to remove the HP OpenView Operations agent from the SESA Manager computer.

To uninstall the HP OpenView Operations agent from the SESA Manager computer

- 1 On the HP OpenView Operations management server, log on to HP OpenView Operations for Windows using the appropriate privileges.
- 2 On the Windows taskbar, click **Start > Settings > Control Panel > Add/Remove Programs**.
- 3 In the Add/Remove Programs window, click **HP OpenView Operations for Windows agent**.
- 4 Click **Remove**, then click **Yes** when you are prompted to remove the software.

Uninstalling the Symantec Relay for HP OpenView Operations software from a Windows computer

If the Symantec Relay for HP OpenView Operations is installed on a computer running the Windows operating system, you can uninstall the software using the Windows Add/Remove Programs feature.

Uninstall the Symantec Relay for HP OpenView Operations software from a Windows computer

After you uninstall the software using the Windows Add/Remove Programs feature, you must also delete all SESA component configuration items in HP OpenView Operations for Windows.

To uninstall the Symantec Relay for HP OpenView Operations software from a Windows computer

- 1 On the HP OpenView Operations management server, log on to HP OpenView Operations for Windows.
- 2 On the Windows taskbar, click **Start > Settings > Control Panel > Add/Remove Programs**.
- 3 In the Add/Remove Programs window, click **Symantec Relay for HP OpenView Operations**.
- 4 Click **Remove**, then click **Yes** when you are prompted to remove the software.

To delete the SESA component configuration items in HP OpenView Operations for Windows

- 1 On the HP OpenView Operations management server, log on to HP OpenView Operations for Windows using an account that has administrative privileges to the SESA Manager.

- 2
- On the Windows taskbar, click **Start > Programs > HP OpenView > Console**.
- 3
- In the HP OpenView Operations for Windows Console, delete the following SESA component configuration items:
- SESA Servers node group
- SPI for SESA Tool group
- SPI for SESA policy group
- SESA_SPI_SNMP_alerts policy
- SESA Administrators user role

Uninstalling the Symantec Relay for HP OpenView Operations software from a UNIX computer

If the Symantec Relay for HP OpenView Operations is installed on a computer running the Sun Solaris or HP-UX operating system, you can uninstall the software by command line.

Uninstall the Symantec Relay for HP OpenView Operations software from a UNIX computer

After you uninstall the software, you must also delete the SESA component configuration symbols in the HP OpenView Operations for UNIX windows.

Note: To uninstall the software, you must change to a user account with root privileges.

Table 2-4 lists the SESA component configuration symbols that you delete from HP OpenView Operations for UNIX.

Table 2-4 SESA component configuration symbols






Symbol	Description
	SESA Administrators

Table 2-4 SESA component configuration symbols

Symbol	Description
	SESA Console
	SESA Servers
	SESA SPI
	SESA Messages

To uninstall the Symantec Relay for HP OpenView Operations from a UNIX computer

- 1 On the HP OpenView Operations for UNIX management server, open the UNIX Console or Terminal window.
- 2 In the UNIX Console or Terminal window, at the command prompt, type **-su** to change to a super user account, then log in using the appropriate password.
- 3 At the prompt, if necessary, change to the directory that contains the swremove script.
- 4 Type the following script:
swremove SESA_SPI @ <Host computer name>
<Host computer name> is the host name of the HP OpenView Operations management server.

To delete the SESA component configuration symbols from the HP OpenView Operations for UNIX windows

- 1 On the HP OpenView Operations for UNIX management server, log in to HP OpenView Operations for UNIX using appropriate administrative privileges.
- 2 In the VPO Node Bank window, on the Window menu, click **Node Group Bank**.
- 3 In the VPO Node Group Bank window, click the **SESA Servers** symbol, then on the Actions menu, click **Node Group > Delete**.
- 4 In the VPO Node Bank window, on the Window menu, click **Message Group Bank**.
- 5 In the Message Group Bank window, click the **SESA Messages** symbol, then on the Actions menu, click **Message Group > Delete**.
- 6 In the VPO Node Bank window, on the Window menu, click **Application Group Bank**.
- 7 In the Application Bank window, click the **SESA SPI Application group** symbol, then on the Actions menu, click **Application > Delete**.
The SESA Console tool is also deleted.
- 8 In the VPO Node Bank window, on the Window menu, click **User Profile Bank**.
- 9 In the User Profile Bank window, click the **SESA Administrators** symbol, then on the Actions menu, click **User Profile > Delete**.
- 10 In the VPO Node Bank window, on the Window menu, click **Message Source Templates**.
- 11 In the Message Source Templates window, under Template Groups, double-click **SESA_SPI**, select the SNMP template, then click **Delete From All**.
The SNMP template is deleted.
- 12 Click **SESA_SPI**, then click **Delete From All**.
The SESA_SPI template group is deleted.

Testing, using, and troubleshooting the Symantec Relay for HP OpenView Operations

This chapter includes the following topics:

- [Testing Symantec Relay for HP OpenView Operations operation](#)
- [Launching the SESA Console in HP OpenView Operations](#)
- [Troubleshooting the Symantec Relay for HP OpenView Operations](#)

Testing Symantec Relay for HP OpenView Operations operation

You can verify that the Symantec Relay for HP OpenView Operations software is operating and that the SESA Manager and HP OpenView Operations are configured correctly to relay and receive alerts respectively.

To verify installation and configuration, perform the following procedures:

- [Verifying that SESA can successfully generate an alert](#)
- [Verifying that SESA configuration components appear in the HP OpenView Operations Console](#)
- [Verifying that SESA alerts appear in the HP OpenView Operations Console](#)

Verifying that SESA can successfully generate an alert

You can create a simple alert configuration in SESA, and then trigger it to make sure that SESA can successfully generate alerts. The alert configuration that you create can be triggered by any events that occur in SESA.

Verify that SESA can successfully generate an alert

Using the Create a new Alert Configuration Wizard, you can create an alert configuration, then test it. The simplest way to trigger an alert is to refresh the Web browser, then log on to the SESA Console again. This causes SESA to generate a Successful Servlet Access event, which you can view in the SESA Console. You can also view the resulting alert report. After you test the alert, you can delete the alert configuration.

To create a test alert configuration

- 1 In the SESA Console, on the Alerts view tab, on the toolbar, click the Alert Configurations icon.
- 2 In the Alert Configurations window, on the toolbar, click **New (+)**.
- 3 In the initial dialog box of the Create a new Alert Configuration Wizard, click **Next**.
- 4 In the General dialog box, select the following:

Alert Configuration name	All Events Test Alert
Alert description	This alert is triggered by any events that occur in SESA
Alert severity	2 - Warning

Leave the remaining options at their default settings.

- 5 Click **Next**.
- 6 Click **Next** in each subsequent dialog box to leave the default settings until you see the Additional Notifications dialog box.
- 7 In the Additional Notifications dialog box, click **Click here to enable SNMP trap message responses for this alert**, then click **Next**.
- 8 In the Alert Configuration Summary dialog box, click **Finish** to create the alert configuration.
- 9 When you see the word Success under the status column, click **Close**.
- 10 In the Alert Configurations window, verify that All Events Test Alert shows in the left pane.

To trigger an alert to verify that SESA can successfully generate it

- 1 In the Web browser containing the SESA Console, click the Refresh icon.
 - 2 Log on to the SESA Console again.
 - 3 In the SESA Console, on the Events view tab, in the left pane, under Global Reports, click **All events**.
 - 4 In the right pane, verify that a Successful Servlet Access event with a severity of 2 is showing.
 - 5 On the Alerts view tab, in the left pane, click **All alerts**.
 - 6 In the right pane, verify that your alert configuration, for example, All Test Events Alert, is showing, and that the Response State is Success.
- A successful response state indicates that the SNMP trap was sent.

Verifying that SESA configuration components appear in the HP OpenView Operations Console

The Symantec Relay for HP OpenView Operations installs a number of SESA configurations in HP OpenView Operations. After you install the Symantec Relay for HP OpenView Operations software, make sure that the configurations show in the HP OpenView Operations Console.

Verify that SESA configuration components appear in the HP OpenView Operations Console

To verify that SESA configurations show in the HP OpenView Operations Console, do the following as necessary:

- Verify that SESA configuration components appear in the HP OpenView Operations for Windows Console.
- Verify that SESA configuration components appear in the HP OpenView Operations for UNIX Console.

To verify that SESA configuration components appear in the HP OpenView Operations for Windows Console

- 1 On the HP OpenView Operations management server, log on to HP OpenView Operations for Windows using the appropriate privileges.
- 2 On the Windows taskbar, click **Start > Programs > HP OpenView > Console**.

- 3 In the HP OpenView Operations Console, in the service tree pane, do the following:
 - Expand **Nodes** to verify that SESA Servers appears under it.
 - Expand **Tools**, then under Tools, click **SPI for SESA** to verify that the Launch SESA Console tool appears in the main view.
 - Expand **Policy Management > Policy groups**, then under Policy groups, click **SPI for SESA** to verify that the SESA_SPI_SNMP_Alerts policy appears in the main view.

To verify that SESA alerts appear in the HP OpenView Operations for UNIX Console

- 1 On the HP OpenView Operations for UNIX management server, log in to HP OpenView Operations for UNIX using appropriate administrative privileges.
- 2 In the VPO Node Bank window, on the Window menu, click **Node Group Bank**.
- 3 In the VPO Node Group Bank window, verify that the SESA Servers symbol appears.
- 4 In the VPO Node Bank window, on the Window menu, click **Message Group Bank**.
- 5 In the Message Group Bank window, verify that the SESA Messages symbol appears.
- 6 In the VPO Node Bank window, on the Window menu, click **Application Group Bank**.
- 7 In the Application Bank window, verify that the SESA SPI symbol appears.
- 8 In the Application Bank window, double-click **SESA SPI**, then verify that the Application Group: SESA SPI window contains the Launch SESA Console symbol.
- 9 In the VPO Node Bank window, on the Window menu, click **User Profile Bank**.
- 10 In the User Profile Bank window, verify that the SESA Administrators symbol appears.
- 11 In the VPO Node Bank window, on the Window menu, click **Message Source Templates**.
- 12 In the Message Source Templates window, under Template Groups, verify that the SESA_SPI template group appears.
- 13 Click **SESA_SPI**, then in the right pane, verify that Trap SESA_SPI_SNMP_Alerts SNMP Alert Interceptor appears.

Verifying that SESA alerts appear in the HP OpenView Operations Console

You can verify that an alert sent by the Symantec Relay for HP OpenView Operations is displaying correctly in the HP OpenView Operations Console.

Verify that SESA alerts appear in the HP OpenView Operations Console

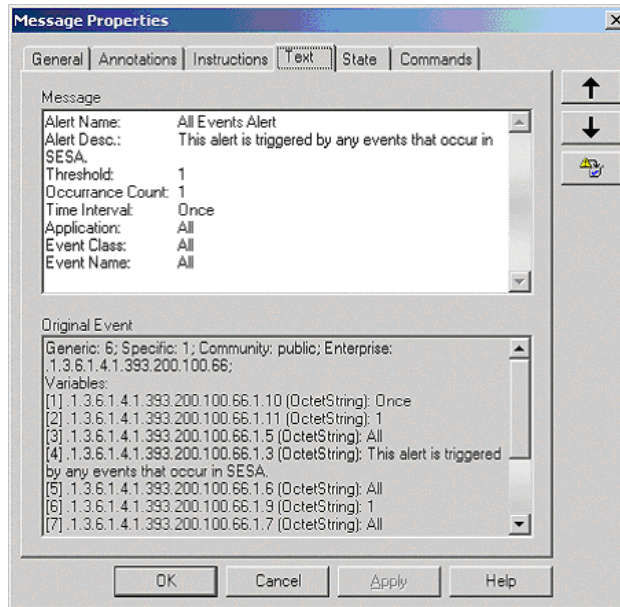
Do the following as necessary:

- Verify that SESA alerts appear in the HP OpenView Operations for Windows Console.
- Verify that SESA alerts appear in the HP OpenView Operations for UNIX Console.

To verify that SESA alerts appear in the HP OpenView Operations for Windows Console

- 1 On the HP OpenView Operations for Windows management server, log on to HP OpenView Operations for Windows using appropriate administrative privileges.
- 2 On the Windows taskbar, click **Start > Programs > HP OpenView > Console**.
- 3 In the HP OpenView Operations Console, in the service tree pane, expand **Nodes**.
- 4 Under Nodes, right-click **SESA Servers**, then click **View > Active Messages**.

- 5 In the main view, right-click the message, then click **Properties**.



- 6 In the Message Properties dialog box, verify that the message contains accurate information from the alert configuration that you created in SESA.
- 7 Click **OK**.

To verify that SESA alerts appear in the HP OpenView Operations for UNIX Console

- 1 On the HP OpenView Operations for UNIX management server, log in to HP OpenView Operations for UNIX using appropriate administrative privileges.
- 2 In the VPO Node Bank window, on the Window menu, click **Message Group Bank**.
- 3 In the Message Group Bank window, click the **SESA Messages** symbol.
- 4 On the Actions menu, click **Message Browser > View Messages of Selected Symbols**.
- 5 In the View Message Browser window, select a message, then click **Details**.
- 6 In the Message Details window, verify that the message contains accurate information from the alert configuration that you created in SESA.
- 7 Click the **Close** button.

Launching the SESA Console in HP OpenView Operations

When the Symantec Relay for HP OpenView Operations is installed successfully, you can launch the SESA Console from within HP OpenView Operations. In this way, you can manage relayed alerts in HP OpenView Operations while tracking the source of the alerts in the SESA Console.

Launching the SESA Console in HP OpenView Operations for Windows

The HP OpenView Operations for Windows Console provides a central location from which to manage relayed alerts and launch the SESA Console to monitor associated reports.

Launch the SESA Console in HP OpenView Operations for Windows

You can use a tool or an operator-initiated command to launch the SESA Console in HP OpenView Operations for Windows.

To launch the SESA Console using the Launch SESA Console tool

- 1 On the HP OpenView Operations for Windows management server, log on to HP OpenView Operations for Windows using appropriate administrative privileges.
- 2 On the Windows taskbar, click **Start > Programs > HP OpenView > Console**.
- 3 In the HP OpenView Operations Console, in the service tree pane, expand **Tools**.
- 4 Under Tools, click **SPI for SESA**.
- 5 In the main view, right-click **Launch SESA Console**, then click **All Tasks > Launch Tool**.
- 6 In the Edit Parameters dialog box, check **SESA Servers**.
- 7 Click **Launch** to open the SESA Console Login window.

To launch the SESA Console using an operator-initiated command

- 1 On the HP OpenView Operations for Windows management server, log on to HP OpenView Operations for Windows using appropriate administrative privileges.
- 2 On the Windows taskbar, click **Start > Programs > HP OpenView > Console**.

- 3 In the HP OpenView Operations Console, in the service tree pane, expand **Nodes**.
- 4 Under Nodes, click **SESA Servers**.
- 5 In the main view, right-click a message, then click **Commands > Start > Operator Initiated** to open the SESA Console Login window.

Launching the SESA Console in HP OpenView Operations for UNIX

The HP OpenView Operations for UNIX Console provides a central location from which to manage relayed alerts and launch the SESA Console to monitor associated reports.

To launch the SESA Console in HP OpenView Operations for UNIX, Netscape browser 4.76 or later must be in the current PATH environment. For more information, go to the Netscape Web site.

In addition, the Sun Java Plug-in version 1.3.1 or later must be configured with the Netscape browser installed. For more information, go to the Java Plug-in Web site.

Launch the SESA Console in HP OpenView Operations for UNIX

You can use an application or an operator-initiated command to launch the SESA Console in HP OpenView Operations for UNIX.

To launch the SESA Console using the Launch SESA Console application

- 1 On the HP OpenView Operations for UNIX management server, log in to HP OpenView Operations for UNIX using appropriate administrative privileges.
- 2 In the VPO Node Bank window, on the Window menu, click **Application Group Bank**.
- 3 In the Application Bank window, double-click **SESA SPI**.
- 4 In the Application Group: SESA SPI window, double-click the **SESA Console** symbol to open the SESA Console Login window.

To launch the SESA Console using an operator-initiated command

- 1 On the HP OpenView Operations for UNIX management server, log in to HP OpenView Operations for UNIX using appropriate administrative privileges.
- 2 In the VPO Node Bank window, on the Window menu, click **Message Group Bank**.
- 3 In the Message Group Bank window, click the **SESA Messages** symbol.

- 4 In the Actions menu, click **Message Browser > View Messages of Selected Symbols**.
- 5 On the View Message Browser window, select a SESA message.
- 6 In the View Message Browser window, on the Actions menu, click **Perform/ Stop Action > Perform Operator-Initiated Action** to open the SESA Console Login window.

Troubleshooting the Symantec Relay for HP OpenView Operations

[Table 3-1](#) lists problems that you may encounter during or after you install the Symantec Relay for HP OpenView Operations. The table also lists possible solutions.

Table 3-1 Symantec Relay for HP OpenView Operations problems and possible solutions

Problem	Possible solution
Alerts from SESA are not appearing in HP OpenView Operations.	<p>Do the following:</p> <ul style="list-style-type: none"> ■ In the SESA Console, verify that the SNMP settings are correctly configured. See “Verifying that SNMP properties are correctly configured in the SESA Console” on page 18. ■ On the SESA Manager computer, verify that SNMP services are installed and started. See “Verifying that SNMP services are installed on the SESA Manager computer” on page 18. ■ In the SESA Console, verify that the SNMP alert notifications are enabled in the alert configuration that you created. See “Configuring alerts in the SESA Manager” on page 28.
The SESA Console does not launch within HP OpenView Operations.	Make sure that the primary DNS suffix is set correctly on the SESA Manager computer. When this suffix is not set correctly, the SESA Console will fail to launch in HP OpenView Operations.

Table 3-1 Symantec Relay for HP OpenView Operations problems and possible solutions

Problem	Possible solution
A change in a SESA configuration is not taking effect or alerts are not being generated in SESA.	<p>Make sure that you did not change the configuration using the SESA Console from within HP OpenView Operations. You can use the SESA Console from HP OpenView Operations for monitoring purposes only. Any configuration changes that you make are not applied.</p> <p>Occasionally, you may need to distribute a configuration change manually in SESA before it can take effect.</p> <p>See “Distributing a configuration change manually in SESA” on page 50.</p>

Distributing a configuration change manually in SESA

When you create an alert configuration, but the changes don’t appear to take effect, you may need to distribute the configuration change manually. To distribute a configuration manually, you must log on to the SESA Console using an account that has access to the System view tab, for example, the SESA Domain Administrator account.

To distribute a configuration change manually in SESA

- Do one of the following to access the SESA Console:
 - In an Internet browser, type **https://<IP address or FQDN of SESA Manager computer>/sesa/ssmc**
 - If you are physically at the SESA Manager computer, on the Windows taskbar, click **Start > Programs > Symantec Enterprise Security > SESA Console**.
- Log on to the SESA Console using a SESA account that has sufficient rights to access the System view tab.
For example, the SESA Domain Administrator account.
- In the SESA Console, on the System view tab, in the left pane, expand **Organizational Units**.
- Under Organizational Units, click **Managers** to activate the Distribute icon on the toolbar.
- On the toolbar, click the **Distribute** icon.
- When the Configure Distribute dialog box prompts you to distribute the configurations, click **Yes**.

Index

A

- agent, HP OpenView Operations for Windows
 - system requirements 20
 - uninstalling 35

alerts

- Alerts view in SESA Console 29
- configuring HP OpenView Operations to receive 24
- configuring in SESA 28
- filtering event class criteria 32
- severities 34
- troubleshooting 49
- verifying appearance in HP OpenView Operations 45
- verifying generation in SESA 42

audience

- for SESA and HP OpenView Operations integration 11
- skill-level requirements 11

C

- CD contents, Symantec Relay for HP OpenView Operations 15
- certification, Smart Plug-Ins 12
- commands, UNIX. *See* scripts
- components, Symantec Relay for HP OpenView 12
- configuration
 - alerts, SESA 28
 - HP OpenView Operations 24
 - Symantec Relay for HP OpenView Operations component in HP OpenView Operations 12

E

events

- creating alert configurations 28
- filtering in alert configuration 32
- processing with Symantec Relay for HP OpenView Operations 14

F

- features, Symantec Relay for HP OpenView Operations 12

H

- HP OpenView Operations
 - configuration 24
 - launching SESA Console
 - UNIX 48
 - Windows 47
 - message severities 34
 - Smart Plug-In certification 12

I

- installation, Symantec Relay for HP OpenView Operations 21

J

- Java Plug-in requirements 48

L

- launching SESA Console 47

N

- Netscape browser requirements 48

O

- operations, testing Symantec Relay for HP OpenView Operations 41
- overview
 - SESA 12
 - Symantec Relay for HP OpenView Operations 12

P

- preinstallation requirements, SNMP service 18

R

- requirements
 - audience 11
 - HP OpenView Operations management server 20
 - launching SESA Console on UNIX platforms 48
 - system, SESA Manager computer 20

S

- scripts
 - swinstall 23
 - swremove 38
- SESA
 - about 12
 - alert severities 34
 - configurations, verifying appearance in HP OpenView Operations 43
 - configuring alerts 28
 - troubleshooting configuration in HP OpenView Operations 50
- SESA Console
 - Alerts view tab 29
 - launching
 - in HP OpenView Operations for UNIX 48
 - in HP OpenView Operations for Windows 47
 - troubleshooting launching 49
- Smart Plug-In 12
- SNMP services
 - configuring in SESA Console 18
 - verifying installation 18
- swinstall 23
- swremove 38
- Symantec Relay for HP OpenView Operations
 - about 12
 - CD contents 15
 - event processing 14
 - installing 21
 - skill level required 11
 - Smart Plug-In certification 12
 - testing 41
 - troubleshooting 49
 - uninstalling 35
- system requirements
 - HP OpenView Operations management server 20
 - launching SESA Console on UNIX platforms 48
 - SESA Manager computer 20

T

- testing, Symantec Relay for HP OpenView Operations 41
- troubleshooting, Symantec Relay for HP OpenView Operations 49

U

- uninstallation
 - Symantec Relay for HP OpenView Operations software 35
 - UNIX platforms 37
 - Windows platforms 36
- UNIX
 - HP OpenView Operations
 - adding SESA Manager node 24
 - launching SESA Console 48
 - Symantec Relay for HP OpenView Operations
 - installation script 23
 - installing 21, 23
 - uninstallation script 38
 - uninstalling 37
- using Symantec Relay for HP OpenView Operations. *See* launching SESA Console

V

- verifying
 - alert generation in SESA 42
 - alerts appearing in HP OpenView Operations 45
 - SESA configuration appearance in HP OpenView Operations 43
 - SNMP services installation 18

W

- Windows
 - HP OpenView Operations
 - adding SESA Manager node 27
 - launching SESA Console 47
 - Symantec Relay for HP OpenView Operations
 - installing 21
 - uninstalling 36
- wizards
 - Create a new Alert Configuration 30
 - Symantec Relay for HP OpenView Operations installation, Windows platforms 21